

Application No. 10/731,606
After Final Office Action of March 30, 2010

9

Docket No.: 60395(49381)

REMARKS

In the Office Action dated March 30, 2010, claims 1-20 and 23-26 are pending and all claims stand rejected. The rejection is made final. Reconsideration is requested at least for the reasons discussed hereinbelow.

Applicant appreciates the courteous interview extended by Examiner Louie to its representative on June 1, 2010. The substance of the discussion is included in the remarks below.

The present invention, as set forth in claim 1, is directed to an image forming apparatus in combination with a sheet having one or a plurality of memories. The image forming apparatus comprises an acquisition unit for acquiring an image signal; an image forming unit for forming an image based on the image signal acquired by said acquisition unit; an encryption key creating unit for creating an encryption key when said acquisition unit acquires the image signal; an encrypting unit for encrypting the image signal with the encryption key created by said encryption key creating unit; a writing unit for writing the encryption key and the encrypted image signal into the one or a plurality of memories on said sheet; a reading unit for reading an encrypted image and encryption key from the sheet; and a decryption unit for decrypting the encrypted image using the encryption key read by the reading unit.

Thus, the image forming apparatus can create an encryption key when receiving an image signal and encrypt the image received, then, write the encrypted image and encryption key to a memory formed on a sheet. The apparatus also can read the encryption key and encrypted image from the sheet and decrypt the encrypted image using the encryption key.

Okamoto fails to teach or suggest an image forming apparatus that can

1. create an encryption key when receiving an image signal and encrypt the image received,
2. write the encrypted image and encryption key to a memory formed on a sheet, and
3. read the encryption key and encrypted image from the sheet and decrypt the encrypted image using the encryption key.

Application No. 10/731,606
After Final Office Action of March 30, 2010

10

Docket No.: 60395(49381)

Claims 1-4, 12, 13, 23 and 24 are rejected under 35 U.S.C. §103(a) over Okamoto et al (US 6,659,353; "Okamoto") in view of Hutchison (US 2003/0145218). Okamoto discloses a method for checking sheets for forgery wherein the sheet is provided with an electronic circuit chip from which information can be read out or written and having visible information.

To the contrary, the present invention is directed to an image forming system designed to restrict copying actions through use of an encryption key system.

Okamoto FIG. 1 shows an electronic chip circuit. FIGs. 2 and 3 show a configuration of a manufacturing apparatus and flow chart for manufacturing a sheet with an electronic sheet. FIGs. 4-6 illustrate a method for detecting a forged sheet. Nowhere is there any suggestion that an image forming apparatus combine these functions. Nowhere is there any suggestion that, by combining these functions, one could provide an image forming system designed to restrict copying actions through use of an encryption key system.

Further, Okamoto states that, during the manufacturing, contents to be printed on the sheet are encrypted [col. 6, lines 42-43]. There is no suggestion that the encryption key be stored in the chip. At Col. 7, lines 47-59, Okamoto teaches using a public key cryptosystem.

Further, at Col. 7, lines 27 *et seq.*, Okamoto states that information uniquely associated with the sheet is stored in the electronic circuit chip. The unique information can include watermark, pattern or the like (col. 8, line 6), security number (col. 8, line 8), bond ID numbers (col. 8, line 13) information concerning size or dimensions of the chip (col. 8, lines 35-40), relative position information (col. 10, lines 17-30), etc. Nowhere is there any suggestion in Okamoto for at least the following elements:

- an encryption key creating unit for creating an encryption key when said acquisition unit acquires the image signal;

- an encrypting unit for encrypting the image signal with the encryption key created by said encryption key creating unit; and

Application No. 10/731,606
After Final Office Action of March 30, 2010

11

Docket No.: 60395(49381)

a writing unit for writing the encryption key and the encrypted image signal into the one or a plurality of memories on said sheet,
as set forth in present claim 1, much less that the image forming unit also comprise:
a reading unit for reading an encrypted image and encryption key from the sheet; and
a decryption unit for decrypting the encrypted image using the encryption key read by the reading unit.

Okamoto discloses "storing encrypted information in an electronic circuit chip on a sheet." However, it fails to teach at least "creating an encryption key when an image signal is acquired" and "writing the encryption key into a memory on a sheet."

Regarding claim 12, Okamoto fails to teach or suggest at least:

a sheet having one or a plurality of memories storing an encryption key;

a memory reading unit for reading the encryption key from the memory on said sheet having one or a plurality of memories when said image reading unit reads the first image; and

a decrypting unit for decrypting the image signal of the first image read by said image reading unit, with the encryption key read by said memory reading unit,

wherein said image forming unit forms the second image based on the image signal decrypted by said decrypting unit on said another sheet.

The Examiner admits that Okamoto fails to teach an encryption key creating unit for creating an encryption key when said acquisition unit acquires the image signal and a step of storing the encryption key in a memory. The Examiner cites Hutchison to make up for this failure of Okamoto. However, Hutchison fails to make up for the deficiencies of Okamoto.

First, it should be noted that, as pointed out above, besides other shortcomings, Okamoto also fails to teach storing the encrypted image signal.

Application No. 10/731,606
After Final Office Action of March 30, 2010

12

Docket No.: 60395(49381)

Hutchison discloses a copying machine. It is not seen how one of ordinary skill in the art would combine a copying machine with a method for checking authenticity of a document with a built-in chip.

Hutchison discloses that 'encryption keys are generated, not in copier 10 (which corresponds to the image forming apparatus of the present invention) but, in an external computer 60 connected to the copier (para. [0024])" and the "external computer 60 maintains decryption keys for individual page images (para. [0030])," etc.

Hutchison discloses creating an encryption key and storing it in the copier memory, in an external computer or in a smart card. Moreover, encrypted data is decrypted by a decryption key read out from the external computer. There is no disclosure or suggestion for storing the encryption key in a memory on a sheet that also contains the image encrypted with the encryption key. The only disclosure or suggestion in Hutchison for storing both the encrypted image and the encryption key together is storing them in the copier memory. Thus, Hutchison fails to teach or suggest "creating an encryption key and writing it into a memory on a sheet." The advantage of the present invention is that the encrypted image may be transported to various locations and, yet, a decrypted image can be printed at any location having an image forming apparatus, as claimed, because the encrypted image and encryption key are together on the transportable sheet.

Thus, Hutchison also fails to teach or suggest

- i. an image forming apparatus in combination with a sheet having one or a plurality of memories;
- ii. a writing unit for writing the encryption key into and the encrypted image signal into the one or a plurality of memories on said sheet;
- iii. an image forming unit forms a first image based on the image signal encrypted by said encrypting unit on a sheet having one or a plurality of memories; and

Application No. 10/731,606
After Final Office Action of March 30, 2010

13

Docket No.: 60395(49381)

iv. said image forming unit forms a second image on said sheet having one or a plurality of memories based on the image signal decrypted by said decrypting unit with the encryption key read by said memory reading unit when the first image is read.

Although Hutchison describes an encryption key stored in a memory, there is not even a hint of a suggestion that the memory for storage of the encryption key be contained in a sheet bearing the encrypted image.

Thus, Hutchison also fails to teach or suggest at least the following claimed elements of claim 1:

an image forming apparatus in combination with a sheet having one or a plurality of memories;

a writing unit for writing the encryption key and the encrypted image signal into the one or a plurality of memories on said sheet;

a reading unit for reading an encrypted image and encryption key from the sheet; and

a decryption unit for decrypting the encrypted image using the encryption key read by the reading unit;

or at least the following claimed elements of claim 12:

an image forming apparatus in combination with a sheet having one or a plurality of memories storing an encryption key;

a memory reading unit for reading the encryption key from the memory on said sheet having one or a plurality of memories when said image reading unit reads the first image; and

a decrypting unit for decrypting the image signal of the first image read by said image reading unit, with the encryption key read by said memory reading unit.

wherein said image forming unit forms a second image based on the image signal decrypted by said decrypting unit on said another sheet.

Application No. 10/731,606
After Final Office Action of March 30, 2010

14

Docket No.: 60395(49381)

Thus, it is not seen how any combination of Okamoto and Hutchison would suggest the presently claimed invention to one of ordinary skill in the art.

The dependent claims are patentable for at least the same reasons as discussed above.

Further, regarding claim 2, neither Okamoto nor Hutchison even suggest that the encryption key be stored in a memory on the sheet. Thus, it is not seen how any combination of Okamoto and Hutchison would suggest "a memory reading unit for reading the encryption key from memory when said image reading unit reads the image," as claimed herein.

Further, regarding claim 3, it is not seen how any combination of Okamoto and Hutchison would suggest "said writing unit writes the encryption key and the information acquired or created by said information acquiring/creating unit into the same memory, or different memories on said sheet having one or a plurality of memories," as claimed herein.

Further, regarding claims 4 and 13, it is not seen how any combination of Okamoto and Hutchison would suggest "said memory reading unit reads the encryption key and information about the image encrypted with the encryption key from the same or different memories on said sheet having one or a plurality of memories when said image reading unit reads the image, and said image forming apparatus further comprises a display unit for displaying the information read by said memory reading unit," as claimed herein.

Further, regarding claim 23, it is not seen how any combination of Okamoto and Hutchison would suggest "sheet comprises a first memory containing an encryption key and a second memory containing an encrypted image," as claimed herein.

Further, regarding claim 24, it is not seen how any combination of Okamoto and Hutchison would suggest "said memory reading unit reads the encryption key and information about the

Application No. 10/731,606
After Final Office Action of March 30, 2010

15

Docket No.: 60395(49381)

image encrypted with the encryption key from said first memory on said sheet when said image reading unit reads the image, and said image forming apparatus further comprises a display unit for displaying the information read by said memory reading unit,” as claimed herein.

It is not seen how any combination of Okamoto and Hutchison would provide the presently claimed invention. Thus, it is not seen how the presently claimed invention would have been obvious to one of ordinary skill in the art in view of any combination of Okamoto and Hutchison.

Claims 5-11, 14-20, 25 and 26 are rejected under 35 U.S.C. §103(a) over Okamoto in view of Imai (US 6,659,353) in further view of Harada et al (US 2003/0007640; “Harada”). Okamoto and Hutchison are discussed in detail above. Claims 5-11, 14-20, 25 and 26 are patentable for at least the same reasons as discussed above. Imai and Harada *fail* to make up for the deficiencies in Okamoto and Hutchison.

Imai has been discussed in detail in previous papers filed by Applicant; see, for example, paper dated December 9, 2008. For example, Imai *fails* to teach or suggest a sheet, on which the encrypted image is formed, the sheet having one or a plurality of memories **in which the encryption key is written**. As aforesaid, Imai *fails* to teach or suggest, for example, at least the following elements of claim 1:

- i. an image forming apparatus including an acquisition unit for acquiring an image signal, and an image forming unit for forming an image based on the image signal acquired by said acquisition unit **on a sheet having one or a plurality of memories;**
- ii. a writing unit for **writing the encryption key into the memory on said sheet having one or a plurality of memories;**
- iii. said image forming unit forms an image based on the image signal encrypted by said encrypting unit **on said sheet having one or a plurality of memories; and**
- iv. wherein said image forming unit **forms an image based on the image signal encrypted by said encrypting unit on said sheet having one or a plurality of memories..**

Application No. 10/731,606
After Final Office Action of March 30, 2010

16

Docket No.: 60395(49381)

Although Imai describes an encryption key stored in a memory, there is not even a hint of a suggestion that the memory for storage of the encryption key be contained in the sheet bearing the encrypted image.

Thus, Imai also fails to teach or suggest at least the following claimed elements of claim 1:

a writing unit for writing the encryption key and the encrypted image signal into the one or a plurality of memories on said sheet;

a reading unit for reading an encrypted image and encryption key from the sheet; and

a decryption unit for decrypting the encrypted image using the encryption key read by the reading unit;

or at least the following claimed elements of claim 12:

a memory reading unit for reading the encryption key from the memory on said sheet having one or a plurality of memories when said image reading unit reads the image; and

a decrypting unit for decrypting the image signal of the image read by said image reading unit, with the encryption key read by said memory reading unit,

wherein said image forming unit forms an image based on the image signal decrypted by said decrypting unit on another sheet;

or at least the following claimed elements of claim 21:

a sheet having one or a plurality of memories containing an encryption key and an encrypted image;

a reading unit for reading an encrypted image signal and encryption key from the sheet; and

an image forming unit for forming an image based on the encrypted image signal and encryption key read by said reading unit.

Application No. 10/731,606
After Final Office Action of March 30, 2010

17

Docket No.: 60395(49381)

Harrada also has been discussed previously. It also fails to teach or suggest, for example:

an image forming apparatus having, for example, a writing unit for writing the encryption key into the memory on said sheet having one or a plurality of memories,

an image reading unit for reading the image formed on said sheet having one or a plurality of memories and a memory reading unit for reading the encryption key from the memory when said image reading unit reads the image,

an information acquiring/creating unit for acquiring or creating information about the image encrypted with the encryption key, wherein said writing unit writes the encryption key and the information acquired or created by said information acquiring/creating unit into the same memory, or different memories on said sheet having one or a plurality of memories, or

a memory reading unit that reads the encryption key and information about the image encrypted with the encryption key from the same memory, or different memories on said sheet having one or a plurality of memories, when said image reading unit reads the image,

as claimed herein.

Thus, it is not seen how the presently claimed invention would have been obvious to one of ordinary skill in the art in view of any combination of Okamoto, Imai and Harada.

In view of the discussion above, Applicant respectfully submits that the pending application is in condition for allowance. An early reconsideration and notice of allowance are earnestly solicited.

Application No. 10/731,606
After Final Office Action of March 30, 2010

18

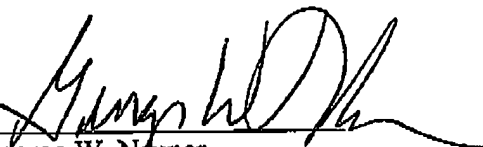
Docket No.: 60395(49381)

If for any reason a fee is required, a fee paid is inadequate or credit is owed for any excess fee paid, the Commissioner is hereby authorized and requested to charge Deposit Account No. 04-1105.

Dated:

18 Jun '10

Respectfully submitted,

By 

George W. Neuner

Registration No.: 26,964

EDWARDS ANGELL PALMER & DODGE
LLP

P.O. Box 55874

Boston, Massachusetts 02205

(617) 517-5538

Attorneys/Agents For Applicant

BOS2 791320.1